Secure Networking for Virtual Machines in the Cloud

IEEE Cluster, PQoSCom workshop
28.9.2012, Beijing
Updated: 1.10.2012 (RTT of HIP)

Miika Komu,
Mohit Sethi,
Ramasivakarthik Mallavarapu,
Heikki Oirola,
Rasib Khan
and
Sasu Tarkoma
Virtualization Security Challenges

- **Multi-tenancy**
  - Two competing companies as tenants for the same host (in a public cloud)
  - Isolate subscriber resources

- **Inter-cloud communication in a hybrid cloud**
  - Hybrid cloud = a private cloud connected with a public cloud
  - Encrypt data flows between the two clouds
  - Cooperation of security mechanisms; unified security?

- **Privacy: process encrypted data**
  - Encrypt the data itself (for example, see CryptDB [1])
Proposed Solution 1 / 2

- Apply HIP [2] in cloud networking
  - Only in inter-cloud (hybrid) or intra-cloud (public) networking
  - Amount of internal traffic can outweigh external
  - Not visible to clients (except for developers and “power” users)
- Because HIP supports...
  - Secure VPN and secure access control (no gateways!)
  - IPv6 interoperability both at application and network layers
  - NAT traversal
  - Mobility (vm migration), multihoming (fault tolerance / load bal.)
  - Site renumbering
  - Incremental deployment
  - Legacy applications
Proposed Solution 2 / 2

Client 1
Client 2
Client 3
...
Client n

Normal HTTP

Load Balancer

HIP-based HTTP

Private/Public IaaS
What is HIP? 1/3

Unmodified TCP/IP Model

TCP/IP with HIP support

Dynamic Binding

Host Identity

= public key
**What is HIP? 2/3**

<table>
<thead>
<tr>
<th>Layer</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Interface</td>
<td>FQDN</td>
</tr>
<tr>
<td>Application Layer</td>
<td>HIT (or LSI), port and proto</td>
</tr>
<tr>
<td>Transport Layer</td>
<td>HIT, port</td>
</tr>
<tr>
<td>HIP Layer</td>
<td>HI</td>
</tr>
<tr>
<td>Network Layer</td>
<td>IP address</td>
</tr>
</tbody>
</table>

HIT = hash(HIT) fitted into IPv6 address, LSI = IPv4-based HI
What is HIP? 3/3

• Compared to SSH...
  – Similar: fingerprint (HIT) calculated from public key
  – Different: IP-layer approach, “leap of faith” optional

• Compared to VPNs
  – Similar: operates above the network layer
  – Different: the gateway is optional (end-to-end)

• Compared to MobileIP
  – Similar: TCP streams survive network handoffs
  – Different: security is built-in (no need for IKE)
On the Performance Measurements

- IaaS cloud n/w
  - EC2
  - OpenNebula
- Multi-tier web service
  - Rubis bidding s/w
  - Latency critical
- Workload generation
  - jmeter, httpperf, iperf
- Centralized database
  - MySQL
  - Elastic Block Storage
- Load balancer
  - HAProxy
  - Round robin
- Comparison point
  - TLS/SSL
Results: Amazon EC2 & Rubis 1/2
Results: Amazon EC2 & Rubis 2/2
Related Work

• VLANs (IEEE 801.Q)
  – In contrast to VLANs, our approach offers stronger security
  – Popa et al [1]: VLANs designed for physical security, not virtual
  – Mukhtarov et al [3]: VLAN vulnerabilities for IaaS clouds

• Comparison to other approaches based on VLANs
  – Netlord [4]; our approach is incrementally deployable
  – Cloud Police [5]; our approach can be integrated with theirs

• Secure Multiparty Communication
  – Fully Homomorphic Encryption (FHE) (encrypted cloud data)
  – Van Dijk et al [6]: FHE is not a holy grail for privacy
Future Work

- Automatize and integrate with, e.g., OpenStack
  - Or why not with clusters?
- Adopt HIP to the browser client side
  - Use case: Chrome (or Amazon Silk Browser)
    - Service owner controls the client (easier deployment)
      - Use HICCUPS extensions [9] for HIP
- Application-layer version of HIP [10]
  - PaaS or SaaS clouds, or with Chrome
Summary

- HIP secures internal traffic in the cloud
  - Mitigates security issues related to multi-tenancy
  - Useful in public and hybrid IaaS clouds
  - Proxy-based approach avoids client deployment hurdles
  - Standardized in the IETF
- Performance evaluation
  - Cloud with HIP support and a bidding web service
  - Offers similar performance as SSL in EC2
  - Verified results also in a private cloud


Questions?

Contact: miika@iki.fi

Host Identity Protocol working group @ IETF:
http://datatracker.ietf.org/wg/hip/charter/

HIP for Linux software project:
http://hipl.hiit.fi/
https://launchpad.net/hipl/